REMARKS

In the Official Action mailed 29 March 2007, the Examiner reviewed claims 1-27. The Examiner found that the application contains claims directed to three patentably distinct species; has objected to the specification; has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §101; has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §101; has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §101; has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §112, second paragraph; has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §112, second paragraph; has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §112, second paragraph; has rejected claim 21 under 35 U.S.C. §112, second paragraph; has rejected claims 1, 8-10, 17-19, 26 and 27 under 35 U.S.C. §103(a); has rejected claims 1, 9, 10, 18, 19 and 27 under 35 U.S.C. §103(a); has provisionally rejected claims 1, 2, 10, 11, 19 and 20 for double patenting; and has indicated that, subject to the above 101, 112, second paragraph, and double patenting rejections, claims 2-4, 11-13 and 20-22 would be allowable over the prior art of record.

Applicant has amended claims 1, 3, 4, 8, 10, 12 and 19, canceled claims 2, 11 and 20, and added new claims 28-31. Claims 1, 3-10, 12-19 and 21-31 are now pending.

Applicant has made clarifying amendments to the independent claims 1, 10 and 19. The amendments clarify the "encrypting" steps and the use of the "conversion array" in the encrypting steps, by reciting the process using a different construction. Method claim 1 is representative, and the modified language includes "providing a particular data random key at the first station, disassembling and veiling the particular data random key by forming a first conversion array seeded by a shared secret and then encrypting the first conversion array to produce a first encrypted data set, where access to the shared secret indicates authenticity of the first station." It is believed that the new language more clearly recites the manner in which the conversion array technology is used to veil a disassemble key, and eliminates the double use of "encrypting" in the clause. Note that the object "encrypted data set" in the new claim language is the encryption of the conversion array, and note that the conversion array veils the disassembled particular data random key. It is believed to more clear to refer to the encryption of the conversion array as an encrypted data set as presented here, than as an "encrypted particular data random key," as used in the claim as filed.

The new independent claims carry this same construction.

The requirement, objection and rejections are respectfully traversed below and reconsideration is requested.

Restriction Requirement

The Examiner has withdrawn Claims 5-7, 13-16 and 22-16 from consideration pending allowance of a generic claim. In light of the amendments herein, it is submitted that claims 1, 10 and 19 from which the withdrawn claims depend are generic, and allowance of the withdrawn claims is requested.

Objection to the Specification

The Examiner has objected to paragraphs [0001] and [0002] of the specification because patent application numbers are missing. Applicant has amended the specification herein to insert the application numbers as suggested by the Examiner.

Accordingly, reconsideration of the objection to the specification as amended is respectfully requested.

Rejection of Claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §101

The Examiner has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §101 because they are not directed to a practical application. Without acquiescing in this basis for rejection, Applicant has amended the independent claims 1, 10 and 19, as suggested by the Examiner, to include the technology for determining whether a match occurs, and continuing further exchanges of messages if a match occurs. Accordingly, a practical application of the invention is recited in the claims. Applicant points out further that the practical application of the invention is clear in the specification.

Accordingly, reconsideration of the rejection of claims 1-4, 8-13, 17-22, 26 and 27 as amended is respectfully requested.

Rejection of Claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §101

The Examiner has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §101 because they are not directed to a practical application. Without acquiescing in this basis for rejection, Applicant has amended the independent claims 1, 10 and 19, as suggested by the

Examiner, to include the technology for determining whether a match occurs, and continuing further exchanges of messages if a match occurs.

In this ground of rejection, the Office Action states "the claimed subject matter does not produce a tangible result because the claim does not recited any step(s) for the second station to authenticate the first station, i.e., the second station does not send a challenge to the first station and receive any response to the challenge from the first station." Reconsideration of this basis for rejection is requested. In particular, the claims recite the steps or logic executed only at the first station. To require specific steps or logic in the second station as indicated by the Examiner would require expanding the claim to include the second station, thereby narrowing the claim, and adding to the burden for showing infringement.

The claims recite the useful components in a single station; and therefore recite a practical application.

As to "mutual" authentication, the technology claimed in independent claims 1, 10, 19 and new independent claims 27-29 participates in that goal by participating in the exchange of messages. The steps at the second station to authenticate the first station are not recited in claims 1, 10, 19 and 27-29. However, the process claimed supports the operation of the second station, by participating in the message exchange needed by the second station to establish that authentication. As described in the specification, the second station relies upon the "third message" for the authentication of the first station.

Applicant adds new claim 31, which recites the steps executed at the first station also in claim 1, and further specifically adds supporting steps executed by the second station. Specifically, the steps of "decrypting the first additional encrypted data set and unveiling and reassembling the additional particular data random key using the additional shared secret, and determining at the second station if the additional particular data random key matches an expected version of the additional particular data random key ..." provide for authentication of the first station by the second station. Applicant asserts however that the claimed invention, as stated in claims 1, 10, 19 and 27-29, has a practical application by simply being capable of participating in the communication process.

Accordingly, reconsideration of the rejection of claims 1-4, 8-13, 17-22, 26 and 27 as amended is respectfully requested.

Rejection of Claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §101

The Examiner has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §101 because they are not directed to a useful process. Without acquiescing in this basis for rejection, Applicant has amended the independent claims 1, 10 and 19, as suggested by the Examiner, to include the technology for determining whether a match occurs, and continuing further exchanges of messages if a match occurs. The continuation of further exchanges in the claims as amended provides a useful result.

Accordingly, reconsideration of the rejection of claims 1-4, 8-13, 17-22, 26 and 27 as amended is respectfully requested.

Rejection of Claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §112, second paragraph

The Examiner has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps relating to matching expected values of decrypted keys at the first station. Without acquiescing in this basis for rejection, Applicant has amended the independent claims 1, 10 and 19, as suggested by the Examiner, to include the technology for determining whether a match occurs, and continuing further exchanges of messages if a match occurs. Accordingly, the allegedly essential elements are now recited in the claims.

Accordingly, reconsideration of the rejection of claims 1-4, 8-13, 17-22, 26 and 27 as amended is respectfully requested.

Rejection of Claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §112, second paragraph

The Examiner has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps relating to acts at the second station. Applicant requests reconsideration of this requirement. In particular, the claims recite all the steps or logic included in the first station, and therefore describe a complete invention. The position that the claim must recite logic executed at remote stations by different systems in order to be complete is believed to be incorrect.

It is sufficient that the recited steps or logic describe technology that participates in a procedure for mutual authentication by supporting the exchange of messages. The technology to implement an invention at a single station is complete technology.

Accordingly, reconsideration of the rejection of claims 1-4, 8-13, 17-22, 26 and 27 as amended is respectfully requested.

Rejection of Claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §112, second paragraph

The Examiner has rejected claims 1-4, 8-13, 17-22, 26 and 27 under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. Regarding claim 1, the allegedly essential steps that are omitted include: "the steps of encrypting, sending and receiving are performed iteratively and for each time, a different data random key is encrypted using a different share secret." As to claims 1, 10 and 19, Applicant has combined the subject matter of dependent claims 2, 11 and 20, which include a following iteration.

Applicant requests reconsideration as to new claims 28-30, which correspond to allowable claims 4, 13 and 22, respectively, and do not recite the following iteration. In particular, the Examiner is taking the position that the sub-combinations recited in the particular claims are not clear outside the setting of the combination described in the specification.

There is no basis in law for this position. The sub-combinations recited in the present claims are useful on their own, and can be applied with or without the allegedly omitted elements of successive iterations. Although it is true that successive iterations might increase the reliability of an authentication session, there is no reasonable basis in law to require the claims to recite further iterations for this reason only.

The technology described in the specification for distributing session-specific symmetric encryption keys relies on this type of mutual authentication and in some embodiments on multiple iterations as noted by the Examiner for very high security. However, this is not the only type of algorithm in which the mutual authentication based on veiled random keys as claimed herein can be applied. Lower security processes may rely on only the single exchange as claimed herein.

Accordingly, reconsideration of the rejection of claims 1-4, 8-13, 17-22, 26 and 27 as amended is respectfully requested.

Rejection of Claim 21 under 35 U.S.C. §112, second paragraph

The Examiner has rejected claim 21 under 35 U.S.C. §112, second paragraph, for a mistake in recited dependency from claim 19 rather claim 20. In light of the amendment of claim 19 to incorporate the subject matter of claim 20, reconsideration is respectfully requested.

Rejection of Claims 1, 8-10, 17-19, 26 and 27 under 35 U.S.C. §103(a)

The Examiner has rejected claims 1, 8-10, 17-19, 26 and 27 under 35 U.S.C. §103(a) as being unpatentable over Bellovin et al. (US 5,241,599) in view of "FIPS 46-3 Data Encryption Standard (DES)." Applicant has amended claims 1, 10 and 19, without prejudice, to incorporate the subject matter of claims 2, 11 and 20 respectively, which the Examiner indicated would be allowable subject matter.

Accordingly, reconsideration of the rejection of claims 1, 8-10, 17-19, 26 and 27 as amended is respectfully requested.

Rejection of Claims 1, 9, 10, 18, 19 and 27 under 35 U.S.C. §103(a)

The Examiner has rejected claims 1, 9, 10, 18, 19 and 27 under 35 U.S.C. §103(a) as being unpatentable over Nessett et al. (US 6,920,559) in view of "FIPS 46-3 Data Encryption Standard (DES)." Applicant has amended claims 1, 10 and 19, without prejudice, to incorporate the subject matter of claims 2, 11 and 20, respectively, which the Examiner indicated would be allowable subject matter.

Accordingly, reconsideration of the rejection of claims 1, 9, 10, 18, 19 and 27 as amended is respectfully requested.

Provisional Rejection of Claims 1, 2, 10, 11, 19 and 20 for Double Patenting

The Examiner has provisionally rejected claims 1, 2, 10, 11, 19 and 20 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 15, 40 and 65 of copending Application No. 10/653,506. Upon allowance of the copending application, Applicant will submit an appropriate Terminal Disclaimer if necessary.

The Examiner' attention is directed to copending Application No. 10/653,503 as well.

Allowable Subject Matter

Subject to the above 101, 112, second paragraph, and double patenting rejections, claims 2-4, 11-13 and 20-22 would be allowable over the prior art of record. Applicant has amended claims 1, 10 and 19 to incorporate the subject matter of claims 2, 11 and 20 respectively, and to address the above rejections.

Applicant has added new claims 28 to 30, which correspond to original allowable claims 4, 13 and 22, respectively. Support for the new claims is therefore found in the original claims 4, 13 and 22.

New claim 31 is added as mentioned above, reciting the process steps executed at both the first and second station. Support for claim 31 is found in Figure X, and throughout the specification.

CONCLUSION

It is respectfully submitted that this application is now in condition for allowance, and such action is requested.

The Commissioner is hereby authorized to charge any fee determined to be due in connection with this communication, or credit any overpayment, to our Deposit Account No. 50-0869 (AIDT 1006-1).

Respectfully submitted,

Dated: 28 June 2007

/Mark A. Haynes/

Mark A. Haynes, Reg. No. 30,846

HAYNES BEFFEL & WOLFELD LLP
P.O. Box 366
Half Moon Bay, CA 94019
(650) 712-0340 phone
(650) 712-0263 fax